压缩大礼包

发表于 2021-01-04 分类于 Challenge， 2019， UNCTF， Misc
Challenge | 2019 | UNCTF | Misc | 压缩大礼包

点击此处获得更好的阅读体验

题目考点

- *zip压缩的缺陷*
- *zip明文攻击*
- *CRC32校验*
- *文件二进制操作*

解题思路

发现是一个名称为1的文件，根据题目提示添加后缀rar，改为1.rar，解压得到2.rar 解压出来的txt无用，下一个压缩包藏在注释里

把十六进制文件复制到HxD保存，得到压缩包命名为3.zip

发现3.zip内有两个文件，解压需要密码，爆破不出来，猜测是伪加密

在kali中直接解压或者通过HxD等软件修改加密位，解压得到4.zip和readme.txt。

打开看readme.txt，只是简单的文字。

4.zip内也有readme.txt，猜测可能是明文攻击,把readme.txt压缩成zip，对比CRC32，确认是明文攻击

使用工具Advanced ZIP Password Recovery进行明文爆破攻击。爆破成功，解压密码为123#qwe!

打开5.zip,发现有好几个txt,内容都比较小，解压需要密码，猜测是CRC32爆破 使用脚本进行CRC32爆破，得到密码welc0meTo7his_un_ctf

打开6.zip,发现有隐藏注释，复制到notepad++或者sublime，设置显示不可见字符

看到内容猜测，可能是摩斯密码，.代表短，-代表长，解密得X233$@F99

解压后得到一张图片，怀疑可能是图种。Binwalk分析有东西。然后直接foremost命令分离

分离出来的压缩包损坏了，修复一下

得到最后一个压缩包，弱密码爆破，四位纯数字，密码是8745

base64解密，得到flag

FLAG

```
1 unctf{D0y0U_1!kE_rAR?}
```

- **本文作者：** CTFHub
- **本文链接：** https://writeup.ctfhub.com/Challenge/2019/UNCTF/Misc/eWnkfFUjzsDBAp9VY9Tx4g.html
- **版权声明：** 本博客所有文章除特别声明外，均采用 BY-NC-SA 许可协议。转载请注明出处！

Challenge # Misc # 2019 # UNCTF
信号不好我先挂了
安妮-起源